REMARKS

This Preliminary Amendment is presented to clearly and distinctly claim the invention. No new matter is added. Entry is respectfully requested.

By this amendment, Claim 22 has been amended. Claims 24-29 have been added. No claims have been cancelled. Hence, Claims 1-29 are pending in the application.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any fee shortages or credit any overages Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP
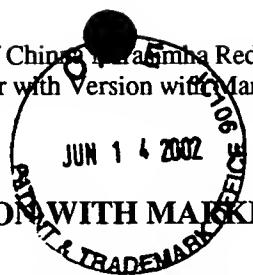
Craig G. Holmes
Reg. No. 44,770

1600 Willow Street
San Jose, CA 95125
(408) 414-1080, ext. 207
Date: June _6_, 2002
Facsimile: (408) 414-1076

6

Application of Chip　Ra鄉mha Reddy PELLACURU, Ser. No. 09/99̇,8, Filed November 27, 2001
Separate Paper with Version with Markings to Show Changes Made to Claims to Accompany Preliminary
Amendment

JUN 1 4 2002

VERSION WITH MARKINGS TO SHOW CHANGES MADE TO CLAIMS

All pending claims are reproduced below in marked-up form, whether or not
amended, for the convenience of examination.

1. 1. (Unchanged) A method for facilitating secure communications among multicast
2. nodes in a telecommunications network, the method comprising the
3. computer-implemented steps of:
4. receiving, from a first node, a first request to store an encryption key, wherein the
5. first request includes an identifier, and wherein the first node uses the
6. encryption key to encrypt data that is multicast with the identifier to a
7. plurality of second nodes;
8. in response to the first request,
9. storing the encryption key;
10. creating and storing an association between the encryption key and the
11. identifier;
12. receiving, from at least one second node of the plurality of second nodes, a second
13. request to obtain the encryption key, wherein the second request includes the
14. identifier;
15. in response to the second request,
16. based on the identifier included in the second request and the association
17. between the encryption key and the identifier, retrieving the
18. encryption key; and
19. sending the encryption key to the at least one second node for use in
20. decrypting the encrypted data.

1. 2. (Unchanged) A method as recited in Claim 1, wherein:
2. a trusted third party performs the steps of receiving the first request, storing the
3. encryption key, creating and storing the association, receiving the second
4. request, retrieving the encryption key, and sending the encryption key;
5. the first node is a router that acts as a multicast originator; and
6. the plurality of second nodes is a plurality of routers that act as multicast receivers.

Application of Chinna Nar⬤ha Reddy PELLACURU, Ser. No. 09/996,94⬤ led November 27, 2001
Separate Paper with Version with Markings to Show Changes Made to Claims to Accompany Preliminary
Amendment

1   3.   (Unchanged) A method as recited in Claim 2, wherein the trusted third party is

2   selected from the group consisting of a certificate authority, a key distribution center,

3   a key exchange authority, and a key exchange center.

4   4.   (Unchanged) A method as recited in Claim 1, wherein the step of receiving the first

5   request includes the step of:

6   receiving a third request to register the encryption key and the identifier.

1   5.   (Unchanged) A method as recited in Claim 1, wherein the steps of creating and

2   storing the association include the step of:

3   registering a certificate that includes the encryption key and the identifier.

1   6.   (Unchanged) A method as recited in Claim 5, further comprising the

2   computer-implemented steps of:

3   in response to the first request, associating an expiration time with the encryption

4   key;

5   in response to the second request, determining based on the expiration time whether

6   the encryption key has expired; and

7   when the encryption key has expired, revoking the certificate.

1   7.   (Unchanged) A method as recited in Claim 1, further comprising the

2   computer-implemented steps of:

3   in response to the first request, associating an expiration time with the encryption

4   key;

5   in response to the second request, determining based on the expiration time whether

6   the encryption key has expired; and

7   when the encryption key has not expired, performing the steps of retrieving and

8   sending the encryption key.

1   8.   (Unchanged) A method as recited in Claim 1, further comprising the

2   computer-implemented steps of:

3   registering the first node; and

4   registering one or more nodes of the plurality of second nodes.

1 9. (Unchanged) A method as recited in Claim 1, further comprising the

2   computer-implemented steps of:

3   generating the encryption key based on an Internet key exchange protocol with the

4   first node.

1 10. (Unchanged) A method as recited in Claim 1, wherein the encryption key is selected

2   from the group consisting of a private key, a shared key, a pseudo-random string of

3   bits, and a pseudo-random string of characters.

1 11. (Unchanged) A method as recited in Claim 1, wherein:

2   the first node uses the encryption key and Internet protocol security (IPsec) to

3   encrypt the data that is multicast; and

4   the at least one second node decrypts the encrypted data based on the encryption key

5   and IPsec.

1 12. (Unchanged) A method as recited in Claim 1, wherein the first request includes a list

2   of authorized second nodes, and further comprising the computer-implemented steps

3   of:

4   in response to the first request, storing the list of authorized second nodes;

5   in response to the second request, determining whether the at least one second node

6   is included in the list of authorized second nodes; and

7   when the at least one second node is included in the list of authorized second nodes,

8   performing the steps of retrieving and sending the encryption key.

1 13. (Unchanged) A method as recited in Claim 1, further comprising the

2   computer-implemented steps of:

3   storing a list of nodes;

4   in response to the first request, determining whether the first node is included in the

5   list of nodes;

6   when the first node is included in the list of nodes, performing the steps of storing

7   the encryption key and creating and storing the association between the

8   encryption key and the identifier.

1   14.   (Unchanged) A method as recited in Claim 1, further comprising the

2   computer-implemented steps of:

3   in response to the first request, associating one or more criteria with the encryption

4   key;

5   in response to the second request, determining based on the one or more criteria

6   whether the encryption key is valid; and

7   when the encryption key is valid, performing the steps of retrieving and sending the

8   encryption key.

1   15.   (Unchanged) A method as recited in Claim 1, wherein the encryption key is an old

2   encryption key, the identifier is an old identifier, and the association is an old

3   association, and further comprising the steps of:

4   in response to the first request, associating one or more criteria with the encryption

5   key;

6   in response to the second request, determining based on the one or more criteria

7   whether the encryption key is valid; and

8   when the encryption key is not valid,

9   receiving a third request to store a new encryption key, wherein the third

10   request includes a new identifier, and wherein the new encryption key

11   is used to encrypt additional data that is multicast with the new

12   identifier to the plurality of second nodes;

13   in response to the third request,

14   storing the new encryption key;

15   creating and storing a new association between the new encryption

16   key and the new identifier;

17   receiving, from at least one additional second node of the plurality of second

18   nodes, a fourth request to obtain the new encryption key, wherein the

19   fourth request includes the new identifier;

20   in response to the fourth request,

21   based on the new identifier included in the fourth request and the new

22   association between the new encryption key and the new

23   identifier, retrieving the new encryption key; and

24   sending the new encryption key to the at least one additional second

25   node for use in decrypting the encrypted data.

1   16.   (Unchanged) A method as recited in Claim 1, wherein the data that the first node

2   encrypts and multicasts is received from a source node.

1   17.   (Unchanged) A method as recited in Claim 1,

2   wherein:

3   the identifier is a session identifier;

4   the encrypted data is multicast with an originator identifier that is based on

5   an identity of the first node;

6   the second request includes an unverified originator identifier; and

7   further comprising the computer-implemented steps of:

8   in response to the first request, associating the originator identifier with the

9   session identifier; and

10   in response to the second request, determining whether the unverified

11   originator identifier is valid based on the originator identifier and

12   informing the at least one second node whether the unverified

13   originator is valid.

1   18.   (Unchanged) A method as recited in Claim 1, wherein:

2   a trusted third party performs the steps of receiving the first request, storing the

3   encryption key, creating and storing the association, receiving the second

4   request, retrieving the encryption key, and sending the encryption key;

5   the first request is encrypted based on a public key that is associated with the trusted

6   third party; and

7   the first request is signed with a private key that is associated with the first node.

1   19.   (Unchanged) A method as recited in Claim 1, wherein a trusted third party performs

2   the steps of receiving the first request, storing the encryption key, creating and storing

3   the association, receiving the second request, retrieving the encryption key, and

4   sending the encryption key, and further comprising the computer-implemented steps

5   of:

6   prior to sending the encryption key,

7   encrypting the encryption key based on a public key that is associated with

8   the at least one second node; and

9   signing the encrypted encryption key with a private key that is associated

10   with the trusted third party.

1   20.   (Unchanged) A method as recited in Claim 1, wherein the identifier is selected from

2   the group consisting of a hostname, an Internet protocol address, a media access

3   control address, an Internet security protocol security parameter index, a first string of

4   pseudo-random bits, a second string of pseudo-random characters, a third string of

5   arbitrary bits, and a fourth string of arbitrary characters.

1   21.   (Unchanged) A method for encrypting communications among multicast nodes in a

2   telecommunications network, the method comprising the computer-implemented

3   steps of:

4   sending an encryption key and an identifier that is associated with the encryption

5   key to an authoritative node that stores the encryption key and identifier and

6   that creates and stores an association between the encryption the encryption

7   key and the identifier;

8   encrypting data based on the encryption key; and

Docket No. 50325-0607 (1640)

9   multicasting the encrypted data with the identifier to one or more receiving nodes,

10   wherein the one or more receiving nodes use the identifier to retrieve the

11   encryption key from the authoritative node and decrypt the encrypted data

12   based on the encryption key.

1   22.   (Once Amended) A method for decrypting [encrypting] <u>encrypted</u> communications

2   among multicast nodes in a telecommunications network, the method comprising the

3   computer-implemented steps of:

4   receiving from an originating node a multicast that includes encrypted data and an

5   identifier;

6   identifying the identifier from the multicast;

7   sending a request that includes the identifier to an authoritative node for an

8   encryption key used by the originating node to encrypt the encrypted data;

9   in response to the request to the authoritative node, receiving the encryption key;

10   and

11   decrypting the encrypted data based on the encryption key.

1   23.   (Unchanged) A method for a certificate authority to facilitate communications based

2   on Internet protocol security (IPsec) among multicast nodes in a telecommunications

3   network, the method comprising the computer-implemented steps of:

4   receiving, at the certificate authority from a first router that acts as a multicast

5   originator, a first request to register an encryption key, wherein the first

6   request includes a multicast session identifier and a list of authorized

7   multicast receivers, and wherein the first router uses the encryption key to

8   encrypt data based on IPsec and multicasts the encrypted data with the

9   multicast session identifier to a plurality of second routers that act as

10   multicast receivers;

11   in response to the first request, the certificate authority creating and storing a

12   multicast session certificate that includes the encryption key, the multicast

13   session identifier, and the list of authorized multicast receivers;

Docket No. 50325-0607 (1640)

14 receiving, at the certificate authority from at least a particular second router of the

15 plurality of second routers, a second request to obtain the encryption key,

16 wherein the second request includes the multicast session identifier;

17 in response to the second request,

18 determining whether the particular second router is included in the list of

19 authorized multicast receivers;

20 when the particular second router is included in the list of authorized

21 multicast receivers,

22 based on the multicast session identifier included in the second

23 request and the multicast session certificate, the certificate

24 authority retrieving the encryption key; and

25 the certificate authority sending the encryption key to the particular

26 second router for use in decrypting the encrypted data based

27 on IPsec.

1 24. (New) A computer-readable medium carrying one or more sequences of instructions

2 for facilitating secure communications among multicast nodes in a

3 telecommunications network, which instructions, when executed by one or more

4 processors, cause the one or more processors to carry out the steps of:

5 receiving, from a first node, a first request to store an encryption key, wherein the

6 first request includes an identifier, and wherein the first node uses the

7 encryption key to encrypt data that is multicast with the identifier to a

8 plurality of second nodes;

9 in response to the first request,

10 storing the encryption key;

11 creating and storing an association between the encryption key and the

12 identifier;

13 receiving, from at least one second node of the plurality of second nodes, a second

14 request to obtain the encryption key, wherein the second request includes the

15 identifier;

16 in response to the second request,

17   based on the identifier included in the second request and the association

18   between the encryption key and the identifier, retrieving the

19   encryption key; and

20   sending the encryption key to the at least one second node for use in

21   decrypting the encrypted data.

1   25.   (New) A computer-readable medium carrying one or more sequences of instructions

2   for encrypting communications among multicast nodes in a telecommunications

3   network, cause the one or more processors to carry out the steps of:

4   sending an encryption key and an identifier that is associated with the encryption

5   key to an authoritative node that stores the encryption key and identifier and

6   that creates and stores an association between the encryption the encryption

7   key and the identifier;

8   encrypting data based on the encryption key; and

9   multicasting the encrypted data with the identifier to one or more receiving nodes,

10   wherein the one or more receiving nodes use the identifier to retrieve the

11   encryption key from the authoritative node and decrypt the encrypted data

12   based on the encryption key.

1   26.   (New) An apparatus for facilitating secure communications among multicast nodes

2   in a telecommunications network, comprising:

3   means for receiving, from a first node, a first request to store an encryption key,

4   wherein the first request includes an identifier, and wherein the first node

5   uses the encryption key to encrypt data that is multicast with the identifier to

6   a plurality of second nodes;

7   means for storing the encryption key, in response to the first request;

8   means for creating and storing an association between the encryption key and the

9   identifier, in response to the first request;

10   means for receiving, from at least one second node of the plurality of second nodes,

11   a second request to obtain the encryption key, wherein the second request

12   includes the identifier;

Docket No. 50325-0607 (1640)

13   means for retrieving the encryption key, in response to the second request and based

14   on the identifier included in the second request and the association between

15   the encryption key and the identifier; and

16   means for sending the encryption key to the at least one second node for use in

17   decrypting the encrypted data, in response to the second request.

1   27.   (New) An apparatus for encrypting communications among multicast nodes in a

2   telecommunications network, comprising:

3   means for sending an encryption key and an identifier that is associated with the

4   encryption key to an authoritative node that stores the encryption key and

5   identifier and that creates and stores an association between the encryption

6   the encryption key and the identifier;

7   means for encrypting data based on the encryption key; and

8   means for multicasting the encrypted data with the identifier to one or more

9   receiving nodes, wherein the one or more receiving nodes use the identifier

10   to retrieve the encryption key from the authoritative node and decrypt the

11   encrypted data based on the encryption key.

1   28.   (New) An apparatus for facilitating secure communications among multicast nodes

2   in a telecommunications network, comprising:

3   a processor;

4   one or more stored sequences of instructions which, when executed by the

5   processor, cause the processor to carry out the steps of:

6   receiving, from a first node, a first request to store an encryption key,

7   wherein the first request includes an identifier, and wherein the first

8   node uses the encryption key to encrypt data that is multicast with the

9   identifier to a plurality of second nodes;

10   in response to the first request,

11   storing the encryption key;

12   creating and storing an association between the encryption key and

13   the identifier;

10

14   receiving, from at least one second node of the plurality of second nodes, a

15   second request to obtain the encryption key, wherein the second

16   request includes the identifier;

17   in response to the second request,

18   based on the identifier included in the second request and the

19   association between the encryption key and the identifier,

20   retrieving the encryption key; and

21   sending the encryption key to the at least one second node for use in

22   decrypting the encrypted data.

1   29.   (New) An apparatus for encrypting communications among multicast nodes in a

2   telecommunications network, comprising:

3   a processor;

4   one or more stored sequences of instructions which, when executed by the

5   processor, cause the processor to carry out the steps of:

6   sending an encryption key and an identifier that is associated with the

7   encryption key to an authoritative node that stores the encryption key

8   and identifier and that creates and stores an association between the

9   encryption the encryption key and the identifier;

10   encrypting data based on the encryption key; and

11   multicasting the encrypted data with the identifier to one or more receiving

12   nodes, wherein the one or more receiving nodes use the identifier to

13   retrieve the encryption key from the authoritative node and decrypt

14   the encrypted data based on the encryption key.

Docket No. 50325-0607 (1640)